CLAIMS OF THE PRESENT INVENTION

1. A data copyright management system for managing the copyright of data which is encrypted and supplied from a database to a user, said data copyright management system having the database and a key control center;

wherein a key for decrypting said encrypted data is supplied from said key control center to said user;

said user uses said key for decrypting when said user displays or edits said data to decrypt said encrypted data; and

said data is re-encrypted when said user stores, copies or transfers said data or data which has been edited.

2. A data copyright management system according to claim 1 wherein said key used in said reencryption is different from said key for decryption.

3. A data copyright management system according to claims 1 or 2 wherein a copyright control program is further used for managing the copyright of said data.

4. A data copyright management system according to claim 3 wherein said data copyright control program is stored in a ROM of a device which said user uses.

5. A data copyright management system according to claim 3 wherein said data copyright control program is stored in system area controlled by an operating system of the device which said user uses.

6. A data copyright management system according to claims 1, 2, 4 or 5 wherein a copyright information which is not encrypted with respect to said data copyright is further used.

7. A data copyright management system according to claim 3 wherein a copyright information which is not encrypted with respect to said data copyright is further used.

8. A data copyright management system according to claims 1, 2, 4, 5 or 7 wherein said copyright information which is not encrypted added to said encrypted data as a copyright information label, said copyright information label being stored, copied or transmitted together with said data in the case where said data is stored, copied or transmitted.

9. A data copyright management system according to claim 3 wherein said copyright information which is not encrypted added to said encrypted data as a copyright information label, said copyright information label being stored, copied or transmitted together with said data in the case where said data is stored, copied or transmitted.

10. A data copyright management system according to claim 6 wherein said copyright information which is not encrypted added to said encrypted data as a copyright information label, said copyright information label being stored, copied or transmitted together with said data in the case where said data is stored, copied or transmitted.

11. A data copyright management system according to claim 8 wherein a digital signature is added to said copyright information label.

12. A data copyright management system according to claim 9 wherein a digital signature is added to said copyright information label.

13. A data copyright management system according to claim 10 wherein a digital signature is added to said copyright information label.

14. A data copyright management system for using data encrypted and supplied from a database to a user, said data copyright management system comprising the database, a key control center and a copyright management center,

wherein said data copyright management system uses secret-key, user information and copyright control program;

said database encrypts the data with first secret-key to distribute the data to a first user via communication network, communication and broadcasting satellite, and record medium;

said first user provides the first user information to said key control center to request the use;

said key control center transfers said first user information to said copyright management center;

said key control center transfers the copyright control program together with said first secret-key and second secret-key to said first user via said communication network;

said first user uses said first secret-key with said copyright control program to decrypt said encrypted data for use; and

said data decrypted is re-encrypted in the case where said decrypted data is stored, copied or transmitted with said copyright control program by using said second secret-key, and uncrypted first user information is added.

15. A data copyright management system according to claim 14 wherein said first secret-key and said second secret-key are disused with said copyright control program, when said decrypted data is copied or transmitted; and

said first user requests for the retransfer of said second secret-key for the reuse of said reencrypted data to said copyright management center so that said second secret-key is retransmitted.

16. A data copyright management system according to claim 15 wherein the copy or transmit of said encrypted data is registered in said copyright management center according to the retransfer of said second secret-key.

17. A data copyright management system according to claim 15 or 16 wherein second user presents said first user information to request the use to said copyright management center;

said copyright management center transfers said second secret-key and third secret-key, and said copyright control program to said second user after confirming the retransfer of said second secret-key to said first user;

said second user decrypts said encrypted data with said copyright control program by using said second secret-key; and

said data is reencrypted and redecrypted with said copyright control program by using said third secret-key when said decrypted data is stored, copied or transmitted.

18. A data copyright management system according to claims 14, 15, or 16 wherein said second secret-key is generated on the basis of any one or more of said first secret-key, said user information, and the usage frequency of said copyright control program with said copyright control program.

19. A data copyright management system according to claim 17 wherein said second secret-key is generated on the basis of any one or more of said first secret-key, said user information, and the usage frequency of said copyright control program with said copyright control program.

20. A data copyright management system for using data encrypted and supplied from a database to a user, said data copyright management

system comprising a database, a key control center and a copyright management center;

wherein said data copyright management system uses secret-key, user information and copyright control program;

first user presents the first user information to the database to request the use of the data;

said database encrypts requested said data by using first secret-key and transfers it to said first user via said communication network together with said first secret-key, second secret-key and said copyright control program;

said key control center transfers said first user information to said copyright management center;

said key control center transfers the copyright control program together with said first and second secret-keys to said first user via said communication network;

said first user decrypts and uses said encrypted data with said copyright control program by using said first secret-key; and

said data decrypted is re-encrypted when said decrypted data is stored,copied or transmitted with said copyright control program by using said second secret-key, and uncrypted first user information is added.

21. A data copyright management system according to claim 20 wherein said first and second secret-keys are disused with said copyright control program when said decrypted data is copied or transmitted;

said first user requests retransfer of said second secret-key for the reuse of the reencrypted data to said copyright management center; and

said second secret-key is retransferred.

22. A data copyright management system according to claim 21 wherein the copy or transmit of said encrypted data is registered in said copyright management center according to the retransfer of said second secret-key.

23. A data copyright management system according to claim 21 or 22 wherein second user presents said first user information to request the use to said copyright management center;

said copyright management center transfers said second secret-key, third secret-key and said copyright control program to said second user after confirming the retransfer of said second secret-key to the first user;

said second user decrypts said encrypted data with said copyright control program by using said second secret-key; and

said data is reencrypted and redecrypted with said copyright control program by using said third secret-key in the case where said decrypted data is stored, copied or transmitted.

24. A data copyright management system according to claims 20, 21, or 22 wherein said second secret-key is generated on the basis of any one or more of said first secret-key, said user information, and the usage frequency of said copyright control program with said copyright control program.

25. A data copyright management system according to claim 23 wherein said second secret-key is generated on the basis of any one or more of said first secret-key, said user information, and the usage frequency of said copyright control program with said copyright control program.

26. A data copyright management system for using data encrypted and supplied from a database to a user, said data copyright management system comprising a database, a key control center and a copyright management center;

said data copyright management system uses secret-key, public-key and private-key;

first user presents first public-key, second public-key and first user information to request the use of the desired data to said key control center;

said database which receives the request for use encrypts said data by using first secret-key, encrypts said first secret-key by using said first public-key, and encrypts second secret-key by using said second public-key;

said encrypted data, said encrypted first secret-key, said encrypted second secret-key and said copyright control program are transmitted to said first user;

said first user decrypts said encrypted first secret-key by using first private-key, decrypts said encrypted data by using said decrypted first secret-key, and decrypts said encrypted second secret-key by using second private-key, with said copyright control program;

said data is encrypted and decrypted with said copyright control program by using the second secret-key in the case where said decrypted data is stored, copied or transmitted.

27. A data copyright management system according to claim 26 wherein said first and second secret-keys are disused with said copyright control program when said decrypted data is copied or transmitted;

said first user who reuses said encrypted data requests for the retransfer of said second secret-key for the reuse of said reencrypted data to said copyright management center; and

said second secret-key is retransferred.

28. A data copyright management system according to claim 27 wherein the copy or transmit of said encrypted data is registered in said copyright management center.

29. A data copyright management system according to claim 27 or 28 wherein second user presents said first user information to request the use to said copyright management center;

said copyright management center transfers said second secret-key, third secret-key, and said copyright control program to said second user after confirming the retransfer of said second secret-key to said first user;

said second user decrypts said encrypted data with said copyright control program by using said second secret-key; and

said data decrypted is reencrypted and redecrypted with said copyright control program by using said third secret-key in the case where said decrypted data is stored, copied or transmitted.

30. A data copyright management system according to claims 26, 27, or 28 wherein said second secret-key is generated on the basis of any one or more of said first secret-key, said user information, and the usage frequency of said copyright control program.

31. A data copyright management system according to claim 29 wherein said second secret-key is generated on the basis of any one or more of said first secret-key, said user information, and the usage frequency of said copyright control program.

32. A data copyright management system for using a plurality of data encrypted each by different secret-keys and supplied from database to a user, said system using a secret-key, user information and a copyright control program, said data copyright management system comprising:

first user obtaining from a copyright management center a plurality of copyright control programs unique to original said plurality of data and a plurality of first secret-keys to decrypt said plurality of original data with a plurality of said first secret-keys;

one or a plurality of second secret-keys being generated with a plurality of copyright control programs unique to said plurality of original data;

wherein said plurality of original data which are used or edited are encrypted with said one or a plurality of second secret-keys with said plurality of copyright control programs unique to said plurality of original data to be stored, copied or transmitted together with the edition process data; and

said plurality of original data or said plurality of edited data encrypted with said one or plurality of second secret-keys are decrypted with said one or plurality of second secret-keys and said plurality of copyright control programs obtained from said copyright management center for second user to use and edit by using said edition process.

33. A data copyright management system according to claim 32 wherein said second secret-key is generated with said copyright control program on the basis of any one or more of said first secret-keys and said user information.

34. A data copyright management system for using data encrypted and supplied from a database to a user, using a crypt key, user information and a copyright control program, comprising:

said user presenting user information to said database;

said database supplying said data encrypted with first crypt key to first user;

said first user generating a second crypt key based on said first crypt key with said copyright control program;

said encrypted data being decrypted by using said first crypt key in the case where said first user uses said encrypted data; and

said decrypted data being reencrypted by using said second crypt key in the case where said first user stores, copies or transmits said decrypted data.

35. A data copyright management system according to claim 34 wherein said crypt key is a secret-key.

36. A data copyright management system according to claim 34 wherein said crypt key is a public-key and a private-key.

37. A digital cash management system for using digital cash encrypted and supplied from a financial organization to first user, comprising:

said financial organization supplying a key for decrypting said encrypted digital cash data to said first user;

said digital cash data being decrypted by using said decrypting key in the case where said first user confirms said digital cash data; and

said data being reencrypted in the case where said first user stores said decrypted digital cash data, in the case where changed digital cash data is stored, or in the case where digital cash data is transmitted to said second user.

38. A digital cash management system according to claim 37 wherein the key used in said reencryption is a crypt key which is different from said decrypting key.

39. A digital cash management system according to claims 37 or 38 wherein a digital cash management program is further used for managing said digital cash.

40. A digital cash management system according to claims 37 or 38 wherein first user information which is not encrypted is further used.

41. A digital cash management system according to claim 39 wherein first user information which is not encrypted is further used.

42. A digital cash management system according to claims 37 or 38 wherein said first user information which is not encrypted is added to said encrypted digital cash data as the first user information label to be stored or transmitted together with said digital cash data in the case where said digital cash data is stored, in the case where changed digital cash data is stored, or in the case where said digital cash data is transmitted to the second user.

43. A digital cash management system according to claim 39 wherein said first user information which is not encrypted is added to said encrypted digital cash data as the first user information label to be stored or transmitted together with said digital cash data in the case where said digital cash data is stored, in the case where changed digital cash data is stored, or in the case where said digital cash data is transmitted to the second user.

44. A digital cash management system according to claim 40 wherein said first user information which is not encrypted is added to said encrypted digital cash data as the first user information label to be stored or transmitted together with said digital cash data in the case where said digital cash data is stored, in the case where changed digital cash data is stored, or in the case where said digital cash data is transmitted to the second user.

45. A digital cash management system according to claim 41 wherein said first user information which is not encrypted is added to said encrypted digital cash data as the first user information label to be stored or transmitted together with said digital cash data in the case where said digital cash data is stored, in the case where changed digital cash data is stored, or in the case where said digital cash data is transmitted to the second user.

46. A digital cash management system according to claim 42 wherein a digital signature is added to said first user information label.

47. A digital cash management system according to claim 43 wherein a digital signature is added to said first user information label.

48. A digital cash management system according to claim 44 wherein a digital signature is added to said first user information label.

49. A digital cash management system according to claim 45 wherein a digital signature is added to said first user information label.

50. A digital cash management system for using digital cash encrypted and supplied from a financial organization to a first user, said system using a crypt key, user information and digital cash management program, comprising:

said first user presenting the first user information to said financial organization;

said financial organization providing said first user with said digital cash data encrypted by the first crypt key;

wherein said first user generates a second crypt key on the basis of said first crypt key with said digital cash management program;

said encrypted digital cash data is decrypted by using said first crypt key in the case where said first user confirms said encrypted digital cash data;

said digital cash data decrypted is reencrypted by using said second crypt key to be stored said first user;

said decrypted digital cash data is reencrypted by using said second crypt key and said digital cash data reencrypted is transmitted to second user together with said first user information in the case where said decrypted digital cash data is transmitted to said second user;

said first user information is presented to said financial organization from said second user;

said financial organization generates said second crypt key based on said first user information and transfers said second crypt key to said second user; and

said second user decrypts said reencrypted digital cash data with said digital cash management program by using said second crypt key which is transferred.

51. A digital cash management system according to claim 50 wherein said crypt key is a secret-key.

52. A digital cash management system according to claim 50 wherein said crypt key is a public-key and a private-key.

53. A digital cash management system for using a digital cash encrypted and supplied from a financial organization to first user, said system using a public-key and a private-key, comprising:

said first user presenting first public-key to said financial organization;

said financial organization encrypting digital cash data with said first public-key to supply to said first user;

said first user decrypting said digital cash data by using first private-key;

second user presenting second public-key to said first user;

said first user encrypting said digital cash data which is decrypted with said second public-key to transfer to said second user; and

said second user decrypting said digital cash data by using second private-key.

54. A video conference data management system for using video conference data encrypted and supplied from first user to second user, comprising:

a key for decrypting said encrypted video conference data being supplied from said first user to said second user;

said encrypted video conference data being decrypted by using said decrypting key in the case where said second user uses said video conference data; and

said data being reencrypted in the case where said second user stores decrypted said video conference data, in the case where edited video conference data is stored, or in the case where said video conference data is transmitted to third user.

55. A video conference data management system according to claim 54 wherein a crypt key used for said re-encryption is different from said decrypting key.

56. A video conference data management system according to claims 54 or 55 wherein a video conference data management program for managing said video conference data is further used.

57. A video conference data management system according to claims 54 or 55 wherein first user information which is not encrypted is further used.

58. A video conference data management system according to claim 56 wherein first user information which is not encrypted is further used.

59. A video conference copyright management system according to claims 54 or 55 wherein said uncrypted first user information is added to said encrypted video conference data as the first user information label which is copied or transmitted together with said video conference data in the case where said video conference data is stored, in the case where the edited video conference data is stored, or in the case where the video conference data is transmitted to third user.

60. A video conference copyright management system according to claim 56 wherein said uncrypted first user information is added to said encrypted video conference data as the first user information label which is copied or transmitted together with said video conference data in the case where said video conference data is stored, in the case where the edited video conference data is stored, or in the case where the video conference data is transmitted to third user.

61. A video conference copyright management system according to claim 57 wherein said uncrypted first user information is added to said encrypted video conference data as the first user information label which is copied or transmitted together with said video conference data in the case where said video conference data is stored, in the case where the edited video

conference data is stored, or in the case where the video conference data is transmitted to third user.

62. A video conference copyright management system according to claim 58 wherein said uncrypted first user information is added to said encrypted video conference data as the first user information label which is copied or transmitted together with said video conference data in the case where said video conference data is stored, in the case where the edited video conference data is stored, or in the case where the video conference data is transmitted to third user.

63. A video conference data management system according to claim 59 wherein a digital signature is added to said first user information label.

64. A video conference data management system according to claim 60 wherein a digital signature is added to said first user information label.

65. A video conference data management system according to claim 61 wherein a digital signature is added to said first user information label.

66. A video conference data management system according to claim 62 wherein a digital signature is added to said first user information label.

67. A video conference data management system for using video conference data encrypted and supplied from first user to second user, said

system using a crypt key, user information, and video conference data management program:

wherein said second user presents second user information to said first user;

said first user supplies to said second user said video conference data encrypted with the first crypt key;

said second user uses said video conference data management program to generate the second crypt key based on said first crypt key;

said encrypted video conference data is decrypted by using said first crypt key in the case where said second user uses said encrypted video conference data; and

said decrypted video conference data is reencrypted by using said second crypt key in the case where said second user stores, copies or transmits said decrypted video conference data.

68. A video conference data management system according to claim 67 wherein said crypt key is a secret-key.

69. A video conference data management system according to claim 67 wherein said crypt key is a public-key and a private-key.

70. A data copyright management apparatus connected for use to a system bus in main body of user terminal, comprising a microprocessor, a read only memory, reading and writing memory and EEPROM connected to a microprocessor bus: